SONICWALL®

Ensuring Cybersecurity in a Mobile-First Workplace

Using a multi-layered security approach to ensure mobile security management

E-BOOK

Introduction

Businesses continue to adapt and fine-tune their mobile strategies. Despite choose your own device (CYOD), corporate-owned, personally enabled (COPE), and company owned, business only (COBO) options, bring your own device (BYOD) still remains very popular and shows no signs of slowing down any time soon.

Mobile device protection requires a multi-layered security approach to provide comprehensive protection against various threats.

Mobile Risks

Mobility and BYOD come with several inherent risks:

- Data breaches through lost, stole or hacked devices
- Malware that could spread from the infected device through the corporate network
- Legal and regulatory issues, especially if the device is lost or stolen and contains sensitive company data
- Lack of compliance, which makes it a challenge to maintain a secure IT environment

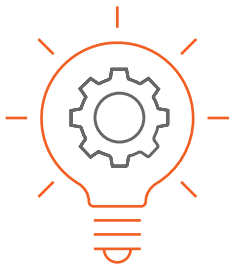
Some companies have tried layering disparate technologies to protect devices and networks independently, but that approach has not been effective.

Security Tools

Today, IT can implement several solid mobile workforce management and mobile security management tools to help secure mobile data and devices:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Mobile Content Management (MCM)
- Mobile Identity and Access Management (IAM)
- Mobile Virtual Private Network (VPN)

Individually, each of these tools has benefits and drawbacks.

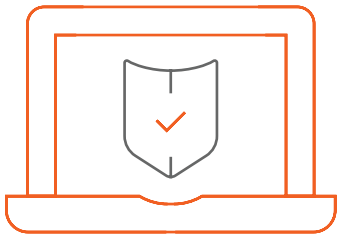


Security tools should improve risk management and help organizations meet regulatory compliance requirements.

Mobile Device Management

Mobile Device Management (MDM) allows IT administrators to monitor, control and secure devices that are used in their organization, regardless of their location. The primary goal of MDM is to ensure the security of sensitive data that is stored and accessed by mobile devices.

MDM offers the ability to wipe a device's data when the device is lost, but it adds IT management and administration of personal devices, which users may resist to protect their own privacy. Data can also be leaked if it's transferred to other devices, because MDM typically creates policies at the user level rather than for applications. In addition MDM can't block information sharing via cloud services or other third-party applications.

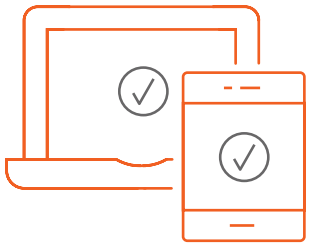


The primary goal of MDM is to ensure the security of sensitive data that is stored and accessed by mobile devices.

Mobile Application Management

Mobile Application Management (MAM) is used to manage and secure mobile applications that are used within an organization. It is focused on securing the application layer rather than the device or network layers. The primary goal of MAM is to ensure the security of corporate data that is accessed and processed by mobile applications.

MAM allows policies to be set at the application level, but not all applications can be managed by MAM. As a result, proprietary application and custom app development may be needed. MAM also may not be popular with mobile users who want application and service choice.



The primary goal of MAM is to ensure the security of corporate data that is accessed and processed by mobile applications.

Mobile Content Management

Mobile Content Management (MCM) can help organizations meet compliance requirements by providing a centralized platform for managing and tracking document access as well as ensuring that sensitive data is not compromised. The primary goal of MCM is to enable organizations to securely manage and share corporate data and documents on mobile devices while maintaining control over how the information is accessed and used.

MCM can be expensive in terms of hardware, software and infrastructure, as well as ongoing maintenance and support costs. Compliance with data privacy laws and industry-specific regulations can be a complex and ongoing process.

The primary goal of MCM is to enable organizations to securely manage and share corporate data and documents on mobile devices while maintaining control over how the information is accessed and used.

Mobile Identity and Access Management

Mobile Identity and Access Management (IAM) is a security framework that enables users to access enterprise resources securely from their mobile devices while also ensuring that these devices comply with organizational security policies and standards. The primary goal of mobile IAM is to provide secure and convenient access to enterprise resources from mobile devices.

Mobile IAM can suffer from poor user experience as well as complexity and compatibility issues. Users may encounter a frustrating experience if they must enter complex passwords or use multi-factor authentication (MFA). Additionally, Mobile IAM can be complex to deploy and manage and may not be compatible with all mobile devices or operating systems, which can make it challenging to manage your mobile environment.

The primary goal of Mobile IAM is to provide secure and convenient access to enterprise resources from mobile devices.

Mobile Virtual Private Network

A mobile virtual private network (Mobile VPN) is a VPN that is specifically designed for mobile devices. Like a regular VPN, the connection creates a secure tunnel between itself and a VPN server and typically uses a mobile device client to facilitate this process. One key benefit of a mobile VPN is that it allows you to use public Wi-Fi networks safely and securely. The primary goal of a mobile VPN is to provide users with a secure and private internet connection as well as greater freedom and flexibility when accessing online content.

Possibly the biggest drawback of using a mobile VPN (or VPN in general) is the performance bottleneck at the VPN server. As all traffic is routed through the VPN server your internet connection may slow down due to the added encryption and processing required to route the traffic. Performance can be limited further on devices with slower processors and less RAM.

The primary goal of a VPN is to provide a secure and private connection between a user's device and the internet.

BYOD Remains Very Popular...

An increasing number of companies are implementing BYOD simply because employees are expected to own a mobile device and use it.

83% of companies have a BYOD policy of some kind.*

*2022 Zippia BYOD statistics

BYOD and Data Protection

Mobile BYOD has become mainstream over the past decade, and this shows no sign of changing. The main inhibitors to BYOD right now are the rules and regulations in the financial services industry. It will be interesting to see how this sector will address requirements to monitor and archive *all* pertinent electronic communications (including on BYOD). Right-to-privacy laws can also complicate BYOD in this environment.

Save for heavily regulated industries, it looks like BYOD is here to stay — at least for the near future. Businesses must carefully consider the potential benefits and risks of BYOD and implement appropriate policies and measures to mitigate risks and ensure a positive user experience.

Financial services employees face strict requirements to monitor and archive *all* pertinent electronic communications.

A Multi-layered Security Approach...

Utilizing a security model with multiple layers of mobile device protection is optimal. At a minimum, security should cover device management, identity and access management, network protection, application protection, and data protection. Listed are the security tools mentioned earlier and how they map to these layers:

- MDM → protects the device and data on the device and helps with compliance
- MAM → protects applications and application data on the device and helps with compliance
- IAM → protects access to digital assets and resources and helps with compliance
- VPN → protects network data and privacy
- MCM → protects access to and sharing of sensitive corporate content on mobile devices and helps with compliance

A multi-layered security solution lowers the risks of BYOD and mobility while giving users what they want — the use of the devices they love with access to the data and applications they need.

Utilizing a security model with multiple layers of mobile device protection is optimal.

Faster, Simpler Mobile Security Management

SonicWall solutions provide IT teams with the level of management and security they need to meet their business requirements. End users get the functionality and features they need and want to do their jobs. SonicWall solutions, IT departments no longer need to buy, install and maintain multiple, disparate mobile solutions from multiple vendors, which ultimately saves time and reduces complexity. SonicWall's Secure Mobile Access (SMA) and Enterprise Mobility Management solutions enable IT teams to:

- Secure and manage endpoint devices, workspaces and containers
- Provide secure access from mobile devices
- Increase overall IT efficiency with powerful granular access control capabilities
- Enable mobile worker productivity while protecting resources from threats

How can I learn more?

Contact us to get in touch with a SonicWall security expert.

Get 30 days to try our Secure Mobile Access with a Free Trial.

Visit our web page, "Secure your mobile access to business data and applications".

SONICWALL

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

Ebook-SMA-JK-8266